ROBBINS GELLER RUDMAN & DOWD LLP
PAUL J. GELLER
120 E. Palmetto Park Road, Suite 500
Boca Raton, Florida 33432
(561) 750-3000
pgeller@rgrdlaw.com

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
ADAM J. LEVITT
55 West Monroe Street, Suite 1111
Chicago, Illinois 60603
(312) 984-0000
levitt@whafh.com

BARNOW AND ASSOCIATES, P.C.
BEN BARNOW
One North LaSalle Street, Suite 4600
Chicago, Illinois 60602
(312) 621-2000
b.barnow@barnowlaw.com

STRANGE & CARPENTER
BRIAN R. STRANGE (103252)
12100 Wilshire Boulevard, Suite 1900
Los Angeles, California 90025
(310) 207-5055
lacounsel@earthlink.net

HERMAN GEREL, LLP
DAVID A. MCKAY
230 Peachtree Street, NW, Suite 2260
Atlanta, Georgia 30303
(404) 880-9500
dmckay@hermangerel.com

Plaintiffs' Steering Committee

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
600 B Street, Suite 1550
San Diego, California 92101
(619) 338-1100
tblood@bholaw.com

CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
GAYLE M. BLATT (122048)
110 Laurel Street
San Diego, California 92101
(619) 238-1811
gmb@cglaw.com

Plaintiffs' Co-Liaison Counsel

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

In re: SONY GAMING NETWORKS AND CUSTOMER DATA SECURITY BREACH LITIGATION, This Document Pertains To: All Actions	MDL No.: 3:11-md-02258-AJB-MDD CLASS ACTION CONSOLIDATED CLASS ACTION COMPLAINT JUDGE: The Honorable Anthony J. Battaglia CTRM: 12 JURY TRIAL DEMANDED

Plaintiffs Scott Lieberman, Kyle Johnson, Arthur Howe, Adam Schucher, Rebecca Mitchell, and Christopher Wilson, individually and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to them and on information and belief as to all other matters, by and through Plaintiffs' Steering Committee and Plaintiffs' Co-Liaison Counsel, bring this Consolidated Class Action Complaint against Sony Corporation of America, Inc.; Sony Computer Entertainment America, LLC; Sony Network Entertainment America, Inc.; Sony Online Entertainment LLC; and Sony Network Entertainment International, LLC (collectively, "Defendants" or "Sony").

INTRODUCTION

1. This Consolidated Class Action Complaint (the "Complaint") is filed pursuant to the August 8, 2011 Transfer Order of the Judicial Panel on Multidistrict Litigation ("JPML"), and Order Following PSC Status Conference, ¶1 [Dkt. No. 63], and presents claims brought against Defendants in the separate cases filed in this District or transferred to this District by the JPML. Unless otherwise ordered by the Court, all claims presented in any case against Defendants subsequently made a part of this multidistrict litigation proceeding shall be deemed to be included in this Complaint.

2. This Complaint is filed to promote judicial efficiency and economy in the adjudication and resolution of pretrial matters and is not intended to effect consolidation for trial of the transferred cases. Neither is this Complaint intended to change the rights of the parties, nor to make those who are the plaintiffs in one case the plaintiffs in another. *See In re Propulsid Prods. Liab. Litig.*, 208 F.R.D. 133, 140-42 (E.D. La. 2002).

3. This nationwide class action arises from one of the largest data security breaches in history. In April 2011, Sony sustained one or more massive security breaches to its computer systems, servers, and databases ("Network").

4. These security breaches (collectively, the "Data Breach"), placed sensitive personal and financial information in the hands of cyber criminals, including customer names, mailing addresses, email addresses, and birth dates, as well as credit and debit card numbers, expiration dates, and security codes, online network passwords, login credentials, answers to security

questions, and other personal information (collectively, "Personal Information"). Plaintiffs and the other Class members provided their Personal Information to Sony when registering/subscribing to the PlayStation Network ("PSN"), Qriocity, and/or Sony Online Entertainment ("SOE") (collectively, "Sony Online Services").

5. Sony owed a legal duty to Plaintiffs and the other Class members to maintain reasonable and adequate security measures to secure, protect, and safeguard their Personal Information stored on its Network. Sony breached that duty by failing to design and implement appropriate firewalls and computer systems, failing to properly and adequately encrypt data, and unnecessarily storing and retaining Plaintiffs' and the other Class members' Personal Information on its inadequately protected Network.

6. Indeed, before the Data Breach, Sony was aware of the security vulnerabilities of its Network, yet failed to warn Plaintiffs and the other Class members of those risks and the susceptibility of its Network to data breaches, such as the Data Breach here; failed to remedy defects in its Network that made it vulnerable to the Data Breach; and continued to encourage consumers to buy Sony hardware and to subscribe to Sony Online Services without warning consumers about the risks inherent in purchasing and relying on Sony's inadequate data security.

7. As the result of Sony's failure to secure its Network, the Data Breach occurred and Plaintiffs' and the other Class members' Personal Information was compromised, placing them at an increased risk of fraud and identity theft, and causing direct financial expenses associated with credit monitoring, replacement of compromised credit, debit and bank card numbers, and other measures needed to protect against fraud arising from the Data Breach. Plaintiffs and the other Class members were also deprived of the unencumbered use of their passwords and their passwords were obtained by a third party without their consent as the result of Sony's failure to adequately and reasonably secure their Personal Information.

8. Additionally, because of its inadequate security and the resulting Data Breach, Sony turned off Sony Online Services for several weeks, causing further damage to Plaintiffs and the other Class members, including the loss of use of Sony Online Services and the full functionality of hardware, including Sony PlayStation 3 ("PS3") consoles and PlayStation Portable ("PSP") devices

and related software and games ("Equipment"). While Sony Online Services were turned off, Plaintiffs and the other Class members continued to be charged for prepaid subscriptions to products or services for specified periods of time accessible through the Network, including, but not limited to Netflix, MLB.TV, and NHL Gamecenter LIVE ("Third Party Services"), despite the inability to use such Third Party Services.

PARTIES

Plaintiffs

9. Scott Lieberman ("Lieberman") resides in Plantation, Broward County, Florida. Plaintiff Lieberman acquired a PS3 in or around early 2007, and created a PSN account shortly thereafter. In order to create his PSN account, Plaintiff Lieberman provided the following personal information to Sony: name, gender, date of birth, mailing address, e-mail address, phone number, and information regarding his American Express credit card account, including the card number, expiration date, security code, and billing address. Plaintiff Lieberman used the PSN to play single and multi-player games online with other PSN users, to purchase and download games, stream prepaid media content from Netflix, and to chat with friends who also used the PSN. Plaintiff Lieberman's PSN account and Netflix account were active on April 16, 2011, and at all relevant times thereafter. Plaintiff Lieberman first learned that his Personal Information had been compromised by the Data Breach through Internet media in or around mid-April 2011. As a result of the Data Breach: (a) Plaintiff Lieberman's Personal Information was stolen, exposing him to a greater risk of identity theft and fraud; and (b) Plaintiff Lieberman was unable to access the PSN, including prepaid Netflix streaming services through the PSN, for approximately 30 days.

10. Kyle Johnson ("Johnson") resides in San Diego, San Diego County, California. Plaintiff Johnson acquired a PS3 in or around the summer of 2007, and created a PSN account shortly thereafter. In order to create his PSN account, Plaintiff Johnson provided the following personal information to Sony: name, gender, date of birth, mailing address, e-mail address, phone number, and credit card information, including the card number, expiration date, security code, and billing address. Plaintiff Johnson has provided such credit card information to Sony regarding three separate credit card accounts—Discover, American Express, and Visa. Plaintiff Johnson used the

PSN to play single and multi-player games online with other PSN users, purchase and download games, stream prepaid media content from Netflix, and to browse the Internet. Plaintiff Johnson's PSN account and Netflix account were active on April 16, 2011, and at all relevant times thereafter. Plaintiff Johnson first learned that his Personal Information had been compromised by the Data Breach through media coverage of the Data Breach and later through an email he received from Sony dated April 27, 2011, regarding the incident. As a result of the Data Breach: (a) Plaintiff Johnson's Personal Information was stolen, exposing him to a greater risk of identity theft and fraud; and (b) Plaintiff Johnson was unable to access the PSN, including prepaid Netflix streaming services, for approximately 30 days. In or around October 2011, two unauthorized charges appeared on Plaintiff Johnson's Visa card.

11. Arthur Howe ("Howe") resides in San Diego, San Diego County, California. Plaintiff Howe acquired a PS3 in or around 2008 and created two new PSN accounts – one for him and one for his minor son. In order to create his PSN accounts, Plaintiff Howe provided the following personal information regarding himself to Sony: name, date of birth, mailing address, email address, phone number, and information regarding his Union Bank debit/credit account and his son's mother's US Bank account, including the card numbers, expiration dates, security codes, and billing addresses. Plaintiff Howe used the PSN mainly to play single and multi-player games online with other PSN users. Plaintiff Howe also used the PSN to purchase and download "map packs," and to stream prepaid media content from Netflix. Plaintiff Howe's PSN accounts and Netflix account were all active on April 16, 2011, and at all relevant times thereafter. Plaintiff Howe first learned that his Personal Information had been compromised by the Data Breach through a letter from Sony dated April 28, 2011. As a result of the Data Breach: (a) Plaintiff Howe's Personal Information was stolen, exposing him to a greater risk of identity theft and fraud; (b) Plaintiff Howe was unable to access the PSN, including prepaid Netflix streaming service for which he was billed $8.99 per month, for approximately 30 days; (c) Plaintiff Howe was forced to close two bank accounts that were compromised; and (d) Plaintiff Howe was forced to purchase a credit monitoring service from freecreditreport.com at a cost of $9.00 per month.

12. Adam Schucher ("Schucher") resides in Surfside, Miami-Dade County, Florida. Plaintiff Schucher acquired a PS3 in or around mid-2008 and created a PSN account shortly thereafter. In order to create his PSN account, Plaintiff Schucher provided the following personal information to Sony: name, gender, date of birth, mailing address, e-mail address, phone number, and information regarding his Citibank Visa credit card account, including the card number, expiration date, security code, and billing address. Plaintiff Schucher used the PSN mainly to purchase and download karaoke songs for *Karaoke Revolution Presents: American Idol* and to chat with friends who also used the PSN. Plaintiff Schucher's PSN account was active on April 16, 2011, and at all relevant times thereafter. Plaintiff Schucher first learned that his Personal Information had been compromised by the Data Breach through Internet media on or around mid-April 2011. As a result of the Data Breach: (a) Plaintiff Schucher's Personal Information was stolen, exposing him to a greater risk of identity theft and fraud; and (b) Plaintiff Schucher was unable to access the PSN for approximately 30 days.

13. Rebecca Mitchell ("Mitchell") resides in East Lansing, Ingham County, Michigan. Plaintiff Mitchell acquired a PS3 in or around May 2009 and created a PSN account. In creating her account, Plaintiff Mitchell provided the following personal information to Sony: name, gender, date of birth, mailing address, e-mail address, and phone number. Subsequently thereto and prior to April 2011, Plaintiff Mitchel provided the PSN with financial information relating to her mother's credit card and her own Visa debit card account, including the card numbers, expiration dates, security codes, and billing addresses. Plaintiff Mitchell used the PSN mainly to purchase, download, and/or access games, karaoke songs for the PlayStation game *Sing Star*, and to browse the Internet. Plaintiff Mitchell's PSN account was active on April 16, 2011, and at all relevant times thereafter. Plaintiff Mitchell first learned that her Personal Information had been compromised by the Data Breach through Internet media on or around April 19, 2011. As a result of the Data Breach: (a) Plaintiff Mitchell's Personal Information was stolen, exposing her to a greater risk of identity theft and fraud; and (b) Plaintiff Mitchell was unable to access the PSN for approximately 30 days.

14. Christopher Wilson ("Wilson") resides in Dallas, Dallas County, Texas. Plaintiff Wilson acquired a PS3 on or around January 2007 and created a PSN account shortly thereafter. In order to create his PSN account, Plaintiff Wilson provided the following personal information to Sony: name, gender, date of birth, mailing address, e-mail address, phone number, and information regarding his Chase Bank Visa debit card account, including the card number, expiration date, security code, and billing address. Plaintiff Wilson used the PSN mainly to play games online with other PSN users, to purchase and download games, and to stream prepaid media content from Netflix. Plaintiff Wilson's PSN account and Netflix account were active on April 16, 2011, and at all relevant times thereafter. Plaintiff Wilson first learned that his Personal Information had been compromised by the Data Breach through an email he received from Sony on or around April 27, 2011. As a result of the Data Breach: (a) Plaintiff Wilson's Personal Information was stolen, exposing him to a greater risk of identity theft and fraud; and (b) Plaintiff Wilson was unable to access the PSN or prepaid Netflix service through the PSN for approximately 30 days.

Defendants

15. Sony Computer Entertainment America LLC ("SCEA") is a Delaware limited liability company with its principal place of business located at 919 East Hillsdale Boulevard, Foster City, California 94404, and conducts business in this District. SCEA is a wholly-owned subsidiary of Sony Corporation of America. On information and belief, SCEA develops, produces, markets, and/or distributes the PS3, PSP, and related hardware and software.

16. Sony Network Entertainment America, Inc. ("SNEA") is a Delaware corporation with its principal place of business located at 550 Madison Avenue, 27th Floor, New York, New York 10022, and conducts business in this District. On information and belief, SNEA functions as Sony's integrated planner and operator of Internet-based content delivery services to owners of Sony televisions, game machines, and other hardware such as the PS3 and PSP, including collecting and managing the Financial, Personal ID, and User Data for the PSN and Qriocity services.

17. Sony Network Entertainment International LLC ("SNEI") is a Delaware limited liability company with its principal place of business located at 6080 Center Drive, Los Angeles, California 90045, and conducts business in this District. On information and belief, SNEI functions

as an operator of Internet-based content delivery services to owners of Sony televisions, game machines, and other hardware such as the PS3 and PSP, including collecting and managing the Financial, Personal ID, and User Data for PlayStation Network and Qriocity services.

18. Sony Online Entertainment LLC ("SOE LLC") is a Delaware limited liability company with its principal place of business located at 8928 Terman Court, San Diego, California 92121, and conducts business in this District. On information and belief, SOE LLC functions as the integrated planner and operator of Sony's online and social network games, including collecting and managing the Financial, Personal ID, and User Data for Sony Online Entertainment services.

19. Sony Corporation of America ("Sony USA") is a Delaware corporation with its principal place of business located at 550 Madison Avenue, 27th Floor, New York, New York 10022, and conducts business in this District, in conjunction with its wholly-owned subsidiaries, including those identified herein. Sony USA is a leading manufacturer of audio, video, communications, and information technology products for the consumer and professional markets.

20. Defendants SCNA, SENA, SNEI, SOE LLC, and Sony USA are sometimes collectively referred to herein as "Sony."

21. At all times relevant to this action, each and every Defendant was an agent and/or employee of each and every other Defendant. In doing the things alleged herein, each and every Defendant was acting within the course and scope of this agency or employment and was acting with the consent, permission and authorization of each of the remaining Defendants. All actions of each Defendant, as alleged herein, were ratified and approved by every other Defendant or its officers or managing agents.

JURISDICTION AND VENUE

22. The Court has subject matter jurisdiction over this class action pursuant 28 U.S.C. §1332(d), because Plaintiffs and the other Class members are of diverse citizenship from one or more Defendants; there are more than 100 Class members nationwide; and the aggregate amount in controversy exceeds five million dollars ($5,000,000.00), excluding interest and costs.

23. Venue is proper in this District under 28 U.S.C. §1391 because Defendants engaged in substantial conduct relevant to Plaintiffs' claims within this District and have caused harm to

Class members residing within this District. Additionally, the class action lawsuits referenced in the caption above have been transferred to this Court for coordinated or consolidated pretrial proceedings per the Transfer Order of the JPML dated August, 8, 2011. Plaintiffs in the transferred actions reserve their rights of remand to the districts from which they were transferred at or before the conclusion of the pre-trial proceedings.

SUBSTANTIVE FACTUAL ALLEGATIONS

A. PlayStation Network, Qriocity, and Sony Online Entertainment

24. Sony developed and launched the PlayStation video game console in 1994. Defendants' current version, the PS3, was released in 2006 and has sold over 47.9 million units worldwide.

25. In 2004, Sony developed and marketed its PSP, which is a hand-held gaming device.

26. One of the key features of the PS3 and PSP devices is their Internet networking capabilities that allow users to connect to the Internet from the devices over a landline connection or "Wi-Fi" – a wireless networking technology allowing the devices to communicate over a wireless signal.

27. Another key feature of the PS3 and PSP is the PlayStation Network ("PSN"). PSN, among other things, allows video game players to engage in multiplayer gaming online (*i.e.*, two individuals can compete against each other in the same video game over an Internet connection as opposed to being in the same room). As of January 25, 2011, PSN had over 69 million users worldwide.

28. In or around February 2011, Defendants launched an entertainment subscription service called "Qriocity" (pronounced "curiosity") that allows users to watch videos, stream music, and upload and manage their personal video and music libraries on their PS3, PSP, and other devices.

29. In or around 1999, SOE LLC, in conjunction with the other Defendants, began developing a service that provides online interactive role-playing games that allowed individuals to compete against each other in the same video game. As of 2011, SOE had over 24.6 million users worldwide.

30. In addition to serving as an online forum or platform for multiplayer gaming and video/music management, Sony Online Services also comprise an online virtual market where PS3, PSP, and online users can purchase videogames, add-on content, demos, themes, game and movie trailers, TV shows, and movies.

31. The PSN also works with various third parties to offer a variety of Third Party Services – such as Netflix, MLB.TV and NHL Gamecenter LIVE – that can be accessed through the PSN. Many users who subscribe to and pay for these Third Party Services can only access them through their PSN account.

32. As of September 2009, there had been over 600 million downloads from the PSN store. Since its launch in February 2011, PS3 and PSP users have participated in video and music streaming through Qriocity.

33. SNEA and SNEI, in conjunction with other of Defendants, manage the PSN and Qriocity services, including overseeing the content delivered to PSN and Qriocity users and managing the Personal Information provided by Plaintiffs and the other Class members as a part of their membership and usage of the PSN and Qriocity services.

34. Sony manages SOE and its services, including overseeing the content delivered to users and managing the Personal Information provided by users as a part of their membership and usage of SOE services.

35. When registering with and/or joining PSN, Qriocity, and/or SOE, users are required to establish an account by providing various personal information to Sony, which Sony, in turn, stores and maintains on its Network.

36. Sony continually monitors and records users' activities, purchases, and usage on the PSN, Qriocity, and SOE, and maintains that usage data in various computer databases on its servers.

37. Users with an account may also create a subaccount for their minor children and others linked to their primary account. During the registration process for these subaccounts, users are required to provide various personal information regarding minor children to Sony, which Sony, in turn, stores and maintains on its Network. Sony continually monitors and records subaccount

users' activities, purchases, and usage on PSN, Qriocity, and SOE and maintains that usage data in various computer databases on its servers.

38. Users with PSN, Qriocity, and/or SOE accounts may also sign up and pay for Third Party Services, such as Netflix, to use on their PSP and PS3 devices. On information and belief, Sony allowed Third Party Services, like Netflix, access to Plaintiffs' and the other Class members' Personal Information to set up Third Party Service accounts and for payment, marketing, and other purposes.

39. On April 1, 2011, SCEA transferred its online PSN and Qriocity service operations to SNEA, including transferring Plaintiffs' and the other Class members' Personal Information to SNEA for handling.

40. As part of that transfer, Sony required all PSN and Qriocity users to agree to a new Terms of Service and User Agreement ("New Agreement") in order to continue using PSN and Qriocity. http://www.qriocity.com/psnlegal/us/tos.html (last visited May 3, 2011).

41. The New Agreement states, in pertinent part, that SNEA collects various data, including Personal Information and usage Data from PSN and Qriocity users as part of their use of Equipment and the PSN and Qriocity services. The New Agreement further states that such data is subject to the terms of SNEA's Privacy Policy.

42. SNEA's Privacy Policy applies to all visitors and users of PSN and Qriocity services, including Plaintiffs and the other members of the Class. It further states:

> [SNEA] strive[s] to take reasonable measures to protect the confidentiality, security, and integrity of the personal information collected from our website visitors. Personal information is stored in secure operating environments that are not available to the public and that are only accessible to authorized employees. In addition, Sony Online Services use industry-standard encryption to prevent unauthorized electronic access to sensitive financial information such as your credit card number. We also have security measures in place to protect the loss, misuse, and alteration of the information under our control. . . . In the event of a security breach, we have procedures in place to protect our consumers' data.

http://www.qriocity.com/psnlegal/us/privacy.html (last visited May 3, 2011).

43. SNEA's Privacy Policy also states that SNEA may share Personal Information and usage Data with SCEA and that such shared content will also be protected according to SCEA's Privacy Policy.

44. SCEA's Privacy Policy states, in pertinent part,

> [SCEA] take[s] reasonable measures to protect the confidentiality, security, and integrity of the personal information collected from our website visitors. Personal information is stored in secure operating environments that are not available to the public and that are only accessible to authorized employees. We also have security measures in place to protect the loss, misuse, and alteration of the information under our control.

http://us.playstation.com/support/privacypolicy/index.htm (last visited May 3, 2011).

45. SOE LLC has a similar Privacy Policy that applies to all users of SOE services. It states:

> In order to provide you with added protection, SOE employs a security technology known as a secure-socket-layer ("SSL") to protect the transmission of payment information to the Site. Unless otherwise specified herein or on the Site where you make a purchase, credit card numbers are used only for payment processing and are not retained for marketing purposes. … [W]e have in place reasonable technical and organizational security measures to protect your Personal Information against accidental or intentional manipulation, loss, destruction, or against unauthorized disclosure or access to the information we collect online.

http://www.soe.com/sonyonline/privacy.vm (last visited May 3, 2011).

B. The Data Breach and Sony's Failure to Disclose

46. On information and belief, during the period April 16-17, 2011, a group of hackers carried out a cyber-attack on Sony's Network. During this attack, the hackers accessed and stole the Personal Information of millions of Sony customers, including Plaintiffs and the other Class members.

47. Sony knew or should have known that its servers, systems, and Network were not secure and left Plaintiffs' and the other Class members' Personal Information vulnerable to attack, theft, and misuse.

48. Sony recklessly, or as a matter of gross negligence, failed to provide adequate security measures—even when earlier threatened with an imminent attack.

49. Moreover, upon learning of the Data Breach, Sony failed to notify Plaintiffs and the other Class members in a timely manner as required by law.

50. On or about April 16, 2011, Sony customers noticed intermittent interruptions to the PSN. Unbeknownst to them, the outages were caused by the massive Data Breach. The Data Breach would not have occurred if Sony properly had maintained, consistent with accepted industry

standards, adequate security measures designed to prevent unauthorized access to Plaintiffs' and the other Class members' Personal Information stored on the Network.

51. On or about April 17, 2011, Sony discovered that PSN and Qriocity user data had been compromised. Sony did not announce its discovery at the time.

52. Three days later, on April 20, 2011, Sony took the PSN and Qriocity offline. Sony did not reveal the truth or the severity of the situation or the reasons for the shutdown to Plaintiffs and the other Class members but, instead, simply advised them that "[w]e're aware certain functions of PlayStation Network are down. We will report back here as soon as we can with more information."[1] Sony's advisory did not mention that a major security data breach had occurred, nor did it inform Plaintiffs and the other Class members that their Personal Information had been compromised or stolen.

53. By taking the PSN and Qriocity off-line, Sony denied Plaintiffs and the other Class members access to their Online Service Accounts, as well as to products and services only available through the PSN and Qriocity for which they had paid Sony and Third-Party Service providers valuable monetary consideration.

54. On April 21, 2011, while the PSN and Qriocity remained off-line, Sony persisted in its failure to tell the truth about the Data Breach to Plaintiffs and the other Class members.

55. Specifically, in a post to Sony's official on-line blog, Patrick Seybold, Sony's Senior Director of Corporate Communications, stated:

> While we are investigating the cause of the Network outage, we wanted to alert you that it may be a full day or two before we're able to get the service completely back up and running. Thank you very much for your patience while we work to resolve this matter. Please stay tuned to this space for more details, and we'll update you again as soon as we can.[2]

---

[1] *See* http://blog.us.playstation.com/2011/04/20/update-on-psn-service-outages-2/, PLAYSTATION BLOG (last visited Jan. 31, 2012).

[2] *See* http://blog.us.playstation.com/2011/04/21/latest-update-on-psn-outage/, PLAYSTATION BLOG (last visited Jan. 31, 2012).

Again, Sony's public disclosures did not inform Plaintiffs and the other Class Members of the Data Breach or that their Personal Information had been compromised or stolen.

56. On April 22, 2011, Sony continued to mislead and misinform Plaintiffs and the other Class members about the cause of and reasons for the "Network outage," the occurrence of the Data Breach, and the attendant damages and risks arising therefrom. Specifically, in another post to Sony's official online blog, Mr. Seybold stated:

> An external intrusion on our system has affected our PlayStation Network and Qriocity services. In order to conduct a thorough investigation and to verify the smooth and secure operation of our network services going forward, we turned off PlayStation Network & Qriocity services on the evening of Wednesday, April 20th. Providing quality entertainment services to our customers and partners is our utmost priority. We are doing all we can to resolve this situation quickly, and we once again thank you for your patience. We will continue to update you promptly as we have additional information to share.[3]

57. Thus, despite possessing actual knowledge of the Data Breach, the severity thereof, and the damages and risks posed to Plaintiffs and the other Class members, Sony elected to hide these important facts about the massive security breach that had compromised the Personal Information of over 77 million of its customers.

58. On April 25, 2011, six days after learning of the Data Breach and shutting down the PSN, Sony again failed to inform Plaintiffs and the other Class members about what had occurred. Specifically, in yet another post to its official on-line blog, Mr. Seybold stated:

> I know you are waiting for additional information on when PlayStation Network and Qriocity services will be online. Unfortunately, I don't have an update or timeframe to share at this point in time.
>
> As we previously noted, this is a time intensive process and we're working to get them back online quickly. We'll keep you updated with information as it becomes available. We once again thank you for your patience.[4]

Again, no word from Sony about the Data Breach or that Plaintiffs' and the other Class members' Personal Information had been compromised or stolen.

---

[3] *See* http://blog.us.playstation.com/2011/04/22/update-on-playstation-network-qriocity-services/, PLAYSTATION BLOG (last visited Jan. 31, 2012).

[4] *See* http://blog.us.playstation.com/2011/04/25/psn-update/, PLAYSTATION BLOG (last visited Jan. 31, 2012).

59. Indeed, Sony did not inform Plaintiffs and the other Class members of the Data Breach or the damages and risks caused by the Data Breach until a full week after Sony learned of it. Specifically, on April 26, 2011, Sony finally issued the following statement:

> Although we are still investigating the details of this incident, we believe that an unauthorized person has obtained the following information that you provided: name, address (city, state, zip), country, email address, birthdate, PlayStation Network/Qriocity password and login, and handle/PSN online ID. It is also possible that your profile data, including purchase history and billing address (city, state, zip), and your PlayStation Network/Qriocity password security answers may have been obtained. If you have authorized a sub-account for your dependent, the same data with respect to your dependent may have been obtained. While there is no evidence at this time that credit card data was taken, we cannot rule out the possibility. If you have provided your credit card data through PlayStation Network or Qriocity, out of an abundance of caution we are advising you that your credit card number (excluding security code) and expiration date may have been obtained.[5]

In conjunction with its belated disclosure, Sony put the burden on Plaintiffs and the other Class members to monitor for damages caused by the Data Breach, cautioning them to watch out for unauthorized use of their credit card data and identity-theft scams. Implicitly recognizing the damage caused by the Data Breach, Sony encouraged Plaintiffs and the other Class members to "remain vigilant, to review your account statements and to monitor your credit reports."[6]

60. Shortly after this "disclosure," Sony admitted that its failure to protect Plaintiffs' and the other Class members' Personal Information gave rise to additional damage. Specifically, in posting answers to "Frequently Asked Questions," Sony included the following questions and answers:

> **11. I want my money back (subscription fee, content) since the PSN/Qriocity was not available.**
>
> While we are still assessing the impact of this incident, we recognize that this may have had financial impact on our loyal customers. We are currently reviewing options and will update you when the service is restored.

---

[5] *See* http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity/, PLAYSTATION BLOG (last visited Jan. 31, 2012).

[6] *Id.*

> **12. There seems to be some games that cannot be played even offline?**
>
> Some games may require access to PSN for trophy sync, security checks or other network functionality and therefore cannot be played offline.

61. At the same time, Sony downplayed a brief interruption in SOE services. Specifically, Sony's answers to "Frequently Asked Questions" regarding the Data Breach included the following question and answer:

> **8. Did SOE experience an attack due to the same reason?**
>
> SOE's services are currently available, but they did experience a service interruption due to an external attack. An investigation is ongoing.[7]

62. On or around April 27, 2011, Sony explained that, with respect to SOE's multiplayer online games, no data was compromised. Specifically, SOE LLC represented that it was "conducting a thorough investigation and, to the best of our knowledge, no customer personal information got out to any unauthorized person or persons."[8]

63. On the morning of May 2, 2011, Sony took SOE off-line and advised Plaintiffs and the other Class members that the action was in response to "an issue that warrants enough concern for us to take the service down immediately."[9]

64. Later that same day, Sony provided additional details. Specifically, in a Customer Service Notification posted on SOE's web site, Sony disclosed – for the first time – that the names, addresses, e-mail addresses, gender, birthdates, phone numbers, log-in names, and hashed

---

[7] *See Hackers stole personal data from PlayStation Network*, http://ingame.msnbc.msn.com/_news/2011/04/26/6538683-hackers-stole-personal-data-from-playstation-network, MSNBC.COM (last visited Jan. 31, 2012).

[8] *See* http://forums.station.sony.com/dcuops3/posts/list.m?topic_id=22096, SONY.COM (last visited Jan. 31, 2012).

[9] *See Sony Online Entertainment servers shut down due to 'issue'*, http://ingame.msnbc.msn.com/_news/2011/05/02/6570322-sony-online-entertainment-servers-shut-down-due-to-issue, MSNBC.COM (last visited Jan. 31, 2012).

passwords of 24.6 million users registered on SOE had been compromised on or around April 16, 2011.[10]

65. On information and belief, the SOE data breach was carried out at the same time, and as part of, the PSN and Qriocity Data Breach.

66. On April 30, 2011, Sony announced that it would compensate PSN and Qriocity users in the United States by offering free identity theft protection service, certain free downloads and online services, and "will consider" helping customers who have to be issued new credit cards.[11]

67. On May 12, 2011, Sony announced that it would compensate SOE users in the United States by offering them free identity theft protection, one month of free service, and certain free in-game (i.e. illusory) bonuses, and currency.

68. Sony's attempts to compensate its PSN, Qriocity, and SOE customers for damages arising from the Data Breach are grossly inadequate.

C. Sony Knew or Should Have Known That Its Networks Were Vulnerable to Attack

69. Sony knew or should have known that its security systems and technologies would leave its Network databases vulnerable to attacks by third-parties. Sony, however, failed to take corrective measures to update its systems and technologies, even after Sony learned of prior security breaches and received a direct threat by a well-known group of hackers to infiltrate its Network.

70. Sony's Network had been compromised by unauthorized users a number of times before the massive April 2011 Data Breach. For example, in May 2009, reports surfaced that

---

[10] *See Sony Confirms Thousands of Credit Cards Stolen During Hack*, http://www.gameinformer.com/b/news/archive/2011/05/02/thousands-of-credit-cards-stolen-during-second-sony-hack.aspx, GAMEINFORMER.COM (last visited Jan. 31, 2012).

[11] *See Sony to restore PSN services, compensate customers*, http://news.cnet.com/8301-31021_3-20058731-260.html?tag=mncol;txt, CNET.COM (last visited Jan. 31, 2012).

unauthorized copies of Sony's customers' credit cards were emailed to an outside account. And, in January 2011, hackers made the PlayStation game *Modern Warfare 2* unplayable through the PSN.

71. Upon information and belief, Sony was not taken by surprise when the Network was breached in April 2011, because Sony knew it had been breached on several prior occasions.

72. Similarly, in late 2010 and early 2011, a 19-year old man named George Hotz also successfully "jailbroke" the PS3 console and created an "exploit"—software or data that takes advantage of a vulnerability in a network to compromise the network and gain control of the system. Hotz's exploit allowed him to modify the PS3 console and use it with other operating systems, like Linux, to play "homebrewed" games. Such modification is relatively common among high-tech gamers, and other console manufacturers, such as Microsoft, silently have acquiesced to the practice. Indeed, earlier versions of the PlayStation console allowed users to modify them without resorting to such jailbreaks.[12]

73. Hotz publicly disclosed his exploit and Sony subsequently sued him for copyright infringement. In response to Sony's lawsuit against Hotz, the hacker collective known as "Anonymous" announced its outrage with Sony and publicly stated that it planned to attack the PSN.[13]

74. Indeed, just two weeks prior to the Data Breach, Anonymous sent the following message to Sony:

> You have abused the judicial system in an attempt to censor information on how your products work . . . Now you will experience the wrath of Anonymous. You saw a hornet's nest and stuck your [expletive] in it. You must face the consequences of your actions, Anonymous style . . . ***Expect us*** (emphasis added).[14]

---

[12] *See* http://en.wikipedia.org/wiki/George_Hotz (last visited Jan. 31, 2012).

[13] *See* http://anonops.blogspot.com/2011/04/opsony.html (Apr. 3, 2011) (last visited Jan. 31, 2012); *see also Anonymous calls out Sony over its treatment of hacker geohot*, http://www.theinquirer.net/inquirer/news/2040139/anonymous-calls-sony-treatment-hacker-geohot, INQUIRER.NET (Apr. 4, 2011) (last visited Jan. 31, 2012).

[14] *See Id.*

75. Despite this direct threat to imminently breach the Network, Sony failed to implement adequate safeguards to protect its Networks, including failing to take steps to protect Plaintiffs' and the other Class members' Personal Information stored on its Networks.

76. Indeed, during a press conference on May 1, 2011, Sony Corporation Chief Information Officer Shinji Hasejima admitted that Sony's Network was not secure at the time of the Date Breach, stating the attack was a "known vulnerability."[15]

D. Sony Failed to Implement Basic Security Measures that Would Have Prevented the Massive April 2011 Security Breach

77. On information and belief, Sony never implemented appropriate security measures and knowingly, recklessly, or as a matter of gross negligence left Plaintiffs' and the other Class members' Personal Information stored on its Network vulnerable to one of the largest cyber-attacks and data thefts in history.

78. Despite Sony's duty to take reasonable steps to secure its Network, it in fact failed to take reasonable and adequate measures to protect Plaintiffs' and the other Class members' Personal Information stored on its Network.

79. On information and belief, among Sony's failures in this respect were its failure to maintain adequate backups and/or redundant systems; failure to encrypt data and establish adequate firewalls to handle a server intrusion contingency; failure to provide prompt and adequate warnings of security breaches; and its unreasonable delay in bringing Sony Online Services back online after the massive Data Breach.

80. As a leader in the computer technology industry, Sony had the ability and know-how to implement and maintain sufficient online security consistent with industry standards.

81. On information and belief, while Sony implemented security systems and technologies to protect its proprietary systems, it failed to employ its expertise as a technology

---

[15] *See Sony's Kaz Hirai addresses PlayStation Network hack*, ENGADGET.COM, http://www.engadget.com/2011/05/01/sonys-kaz-hirai-will-address-playstation-network-hack-at-1am-et/ (last visited Jan. 31, 2012).

leader and other available expertise to implement similar security measures to protect Plaintiffs' and the other Class members' Personal Information stored on its Network.

82. Indeed, on information and belief, Sony invested significant resources, including firewalls, debug programs, and IP address limitations, to protect its confidential proprietary information housed on Sony's "development server," without incorporating the same industry standard safeguards, such as a basic firewall, to its Network storing Plaintiffs' and the other Class members' Personal Information.

83. Sony's decision not to install and maintain appropriate firewalls on its Network deviated from widespread industry practice and standards, including the Payment Card Industry Data Security Standard ("PCI DSS"), which require anyone collecting payment card information to install and maintain a firewall.[16]

84. Moreover, technology security experts at Attrition.org have stated that Sony's lack of encryption when storing Plaintiffs' and the other Class members' personal details and passwords was both "reckless and ridiculous." These experts went on to explain that "even security books from the '80s were adamant about encrypting passwords at the very least."[17]

85. Indeed, on June 8, 2011, Sony's Deputy President, admitted that, at the time of the Data Breach, Sony's Network failed to meet minimum security standards. When asked whether Sony had revised its security systems following the April 2011 Data Breach, Mr. Hirai stated that Sony has "done everything to bring our practices at least in line with industry standards or better."[18]

---

[16] The PCI DSS "is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards." http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard (last visited Jan. 31, 2012).

[17] *See Absolute Sownage: A concise history of recent Sony hacks*, ATTRITION.ORG (June 4, 2011), http://attrition.org/security/rant/sony_aka_sownage.html (last visited Jan. 31, 2012).

[18] *See E3 2011: Sony's Kaz Hirai on the PSN hack*, GUARDIAN.CO.UK (June 8, 2011), http://www.guardian.co.uk/technology/2011/jun/08/e3-2011-sony-psn (last visited Jan. 31, 2012).

E. Industry Experts, Academics, and United States Senators Have Criticized Sony for Failing to Protect the Personal Information of Its Customers

86. In response to the massive April 2011 Data Breach, Sony has represented that it implemented basic measures to defend against new attacks, including the following systems that should have been in place prior to April 2011: automated software monitoring; enhanced data encryption; enhanced ability to detect intrusions to the Network, such as an early-warning system to detect unusual activity patterns; and additional firewalls. Additionally, Sony hired a Chief Information Security Officer.[19]

87. John Bumgarner, Chief Technology Officer of the independent, non-profit research institute United States Cyber-Consequences Unit, found that as of May 10, 2011, the PSN was still vulnerable to attacks. Specifically, unauthorized users could still access internal Sony resources, including security-management tools. Indeed, Bumgarner's research showed that the problems with Sony's systems were more widespread than Sony had acknowledged at that time.[20]

88. Mr. Bumgarner was correct and, as described below, the Sony Pictures Entertainment network was breached on June 2, 2011. LulzSec, the hacking collective that claimed responsibility for that incident, stated that its motivation was to show that Sony lied when it told customers that it had revamped security to protect against the same type of attack that occurred in April 2011.[21]

---

[19] *See Sony Battens Down the Hatches for PlayStation Network, Hiring CISO*, SECURITYWEEK.COM (May 2, 2011), http://www.securityweek.com/sony-battens-down-hatches-playstation-network-hiring-ciso (last visited Jan. 31, 2012); *Sony recruits information security boss after hacking*, REUTERS.COM (Sept. 6, 2011), http://www.reuters.com/article/2011/09/06/us-sony-idUSTRE7851PH20110906 (last visited Jan. 31, 2012).

[20] *See Sony yet to fully secure its networks: expert*, REUTERS.COM (May 13, 2011), http://www.reuters.com/article/2011/05/13/us-sony-idUSTRE74C70420110513 (last visited Jan. 31, 2012).

[21] *See Sony Pictures falls victim to major data breach*, COMPUTERWORLD.COM (June 2, 2011), http://www.computerworld.com/s/article/9217273/SonyPictures_falls_victim_to_major_data_breach (last visited Jan. 31, 2012).

89. Indeed, numerous experts in the field attribute the Sony Pictures data breach to an unsophisticated method of hacking that would not have been successful if Sony had even the most basic security measures in place.

90. For example, Tony Bradley, a PCWorld journalist who covers technology issues, in a June 3, 2011 article entitled, "Sony Hacked Again: How Not To Do Network Security," stated that Sony "seems to ignore compliance requirements and basic security best practices, so it is basically begging to be attacked."[22] Bradley further advised that companies should follow security "best practices and data security compliance requirements"—and in short—"[d]on't be a Sony."[23]

91. Similarly, according to Fred Touchette of AppRiver, an email and web security software provider: "[t]here is no doubt that Sony needs to spend some major effort in tightening up its network security. This latest hack against them was a series of simple SQL Injection attacks against its web servers. This simply should not have happened."[24]

92. Sony's delay in publicly disclosing the Data Breach sparked concern and outrage, causing U.S. Senator Richard Blumenthal (D-Conn.) to condemn Sony's lack of reasonable security measures, stating that: "Sony persists in unconscionably refusing to alert its millions of users on the PlayStation Network proactively, while they remain at serious risk of identity theft and other financial attacks stemming from their personal and financial data having been compromised."[25]

93. Sony customers similarly have expressed their unhappiness and dissatisfaction with Sony's conduct, including the editors of the gamer website IGN.com:

(a) Hilary: "[I]t's disheartening to see a company respond so poorly to the biggest crisis it's faced this console generation . . . Faced with a crisis that

---

[22] *See* Tony Bradley, *Sony Hacked Again: How Not to Do Network Security*, PCWORLD.COM (June 3, 2011), http://www.pcworld.com/businesscenter/article/229351/sony_hacked_again_how_not_to_do_network_security.html (last visited Jan. 31, 2012).

[23] *Id.*

[24] *Id.*

[25] *See* Press Release, Blumenthal Continues to Push Sony over Playstation Data Breach (Apr. 27, 2011), http://blumenthal.senate.gov/newsroom/press/release/blumenthal-continues-to-push-sony-over-playstation-data-breach (last visited Jan. 31, 2012).

> affected its customers, people at Sony ignored compassion, eschewed openness and instead hid in silence . . .While your credit card info may have been exposed to criminals that brought down Sony's service, leaving those loyal to PlayStation in potential financial peril, executives chose to keep their mouths shut . . . Their true selves were revealed – as selfish, greedy, self-centered individuals more concerned with the bottom line than the value of their customer base."

(b) Charles: "It shouldn't have taken this long for Sony to issue a statement about this kind of thing. Customer security should be the number one priority if Sony wants its consumer base to maintain faith in its service."

(c) Tom: "[F]or Sony to wait 6 whole days before holding their hands up to admit 75 million people's PSN details - including credit card details - could have been compromised, is galling to say the least."[26]

F. The Data Breach, Caused by Sony's Improper Conduct, Has Harmed Plaintiffs and the Other Class Members

i. Identity Theft

94. As a result of the Data Breach, cyber-criminals now possess the Personal Information of Plaintiffs and the other Class members. While credit card companies offer protection against unauthorized charges, the process is long, costly, and frustrating. Physical cards must be replaced, credit card information must be updated on all automatic payment accounts, and victims must add themselves to credit fraud watch lists, which substantially impairs victims' ability to obtain additional credit. Immediate notice of the breach is essential to obtain the best protection afforded by these services. As alleged above, Sony failed to provide such immediate notice, thus further exacerbating the damages sustained by Plaintiffs and the other Class members arising from the Data Breach.

ii. Cyber-stalking and Spam

95. Information about Plaintiffs and the other Class Members may also be used to harass or stalk them. And, the threat of "spear phishing"—where details of a person's Usage Data can be used to tailor a "phishing" message that looks authentic, but is actually a ruse to get the consumer to divulge account information—is real.

---

[26] *See The Lobby: PlayStation Network Down, The IGN Editors weigh in on the disastrous breach of the PlayStation Network*, IGN.com (Apr. 26, 2011), http://m.ign.com/articles/1164195 (last visited Jan. 31, 2012).

96. Indeed, at the time it disclosed the Data Breach, Sony cautioned its customers that the breach might lead to email, telephone, and postal scams that ask for personal information.

iii. Lost Use of Sony Online Services

97. The PSN and Qriocity Networks remained offline for almost a month while Sony conducted an audit of its systems to determine exactly how the Data Breach occurred. Similarly, SOE remained offline for more than two weeks. During this prolonged period of downtime, Plaintiffs and the other Class members were unable to access PSN, Qriocity, and SOE; purchase "add-ons" with their virtual wallets; play multi-player online games with others; and to otherwise use online services available through the PSN, Qriocity, and SOE. Plaintiffs and the other Class members were also unable to access and use prepaid Third Party Services, such as Netflix, MLB.TV, and NHL Gamecenter Live.

98. As CNET News explained, the harm caused by the Data Breach and Sony's associated shut down of its PSN as a result thereof was real and expansive:

> While it's free to sign up for PlayStation Network, much of the content that can be downloaded requires a separate subscription to use, and every day that customers can't access that content, they're essentially losing money for something they've prepaid for. And it's not just games.
>
> Other examples include [1] the Netflix app that can be downloaded from the PSN Store and used to access Netflix's Watch Instantly subscription feature; [2] MLB.TV's $100-per-season game package, which lets users watch MLB games on a TV via the PS3; [3] the paid version of Hulu, Hulu Plus and more.
>
> PSN Plus customers are also losing money, since they pay for year or several months blocks of time to access exclusive content from PSN. As of now, they are also unable to play some games they've already downloaded because PSN has to be operational to play.[27]

99. For Plaintiffs and the other Class members, the lost use of pre-paid services significantly lessened the value of their PS3s and PSPs, which they purchased with the expectation that the Network would be accessible 24 hours a day, 7 days a week, for services like online gaming, store purchases, game downloads, and Third Party Services, such as Netflix.

---

[27] *See Five questions for Sony about PSN breach*, CNET.COM (Apr. 27, 2011), http://news.cnet.com/8301-31021_3-20057963-260.html (last visited Jan. 31, 2012).

100. As alleged above, four of Plaintiffs paid a monthly fee for the Third-Party Service Netflix to use through their PS3s but, due to the Data Breach and concomitant outage of the PSN, were unable to use Netflix through their PS3s.

iv. Sony Admits that It Harmed Plaintiffs and the Other Class Members

101. During a press conference on Sunday, May 1, 2011, the Chairman of Sony Computer Entertainment, Kazuo Hirai, readily acknowledged that Sony's failure to protect its customers' Personal Information had harmed its customers:

> Again we like to offer our deepest and sincere apologies for potentially compromising customer data as well as causing great concern and making services unavailable for an extended period of time.

G. Since the April 2011 Data Breach, Sony has Experienced Numerous Other Security Breaches that Call Into Question its Ability to Safeguard its Customers' Personal Information Against Future Attacks

102. On May 18, 2011, just four days after restoring the PSN, Sony took down certain websites that allow PSN users to sign in and restore their passwords. According to Sony, it had discovered, and subsequently fixed, a URL exploit that allowed hackers to change user passwords with the Personal Information stolen during the April 2011 Data Breach.

103. On June 2, 2011, LulzSec announced that it had broken into Sony Pictures Entertainment servers and compromised the personal information of over 1 million individuals, including the names, email addresses, home addresses, telephone numbers, gender, website passwords, user names, dates of birth, associated with their accounts.

104. According to LulzSec, it was able to access and obtain this personal information by using an elementary hacking device known as an "SQL Injection," which it described as "one of the most primitive and common vulnerabilities." The group further claimed that from a "single injection" it "accessed EVERYTHING," and that it was able to do so "easily" and "without the need for outside support or money."[28]

---

[28] *See Sony Pictures website hacked, 1 million accounts compromised*, BGR.COM (June 2, 2011), http://www.bgr.com/2011/06/02/sony-pictures-website-hacked-1-million-accounts-compromised/ (last visited Jan. 31, 2012) (emphasis in original).

105. Even more damning, LulzSec claimed that the data it stole was not encrypted or hidden behind a cryptographic hash tag, but flagrantly stored in plain text.[29] LulzSec also posted on its website certain hijacked Personal Information, including email addresses and passwords, of thousands of Sony customers.[30]

106. Most recently, on October 12, 2011, Sony disclosed that between October 7, 2011 and October 10, 2011, intruders staged a massive attempt to access user accounts on the PSN and other online entertainment services. In response, Sony locked approximately 93,000 user accounts whose identities and passwords were successfully obtained during the October 2011 intrusion.[31]

CLASS ACTION ALLEGATIONS

107. Plaintiffs bring this lawsuit on behalf of themselves and as a class action, pursuant to Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure, on behalf of a proposed class (the "Class"), defined as:

> All persons or entities in the United States that subscribed to the PlayStation Network, Qriocity and/or Sony Online Entertainment service, and suffered a disruption of service and/or breach of security to their personal information beginning on or about April 16, 2011.

108. Excluded from the Class are Defendants, including any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants.

109. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

---

[29] *See Sony LulzSec Hack: What You Need to Know*, PCMAG.COM (June 3, 2011), http://www.pcmag.com/article2/0,2817,2386362,00.asp (last visited Jan. 31, 2012).

[30] *Id.*

[31] *See Sony PlayStation Network Hacked Again, Closes 93,000 Accounts*, ABCNEWS.GO.COM (Oct. 12, 2011), http://abcnews.go.com/blogs/technology/2011/10/sony-playstation-network-hacked-again-closes-93000-accounts/ (last visited Jan. 31, 2012).

110. **Numerosity – Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all members would be impracticable. Upon information and belief, there were approximately 77 million PSN and Qriocity users worldwide impacted by the Data Breach. Approximately 31 million of those 77 million PSN and Qriocity users reside in the United States. In addition, on May 3, 2011, Sony issued a press release announcing that the "personal information from approximately 24.6 million SOE accounts may have been stolen." While the exact number of Class members is currently unknown to Plaintiffs, upon information and belief, Plaintiffs allege that there are, at least, tens of millions of Class members who were damaged by Sony's conduct described herein. The names and addresses of Class members are identifiable through documents maintained by Sony. Ultimately, the sheer number of Class members, who are geographically dispersed around the United States, makes joinder of all members impracticable.

111. **Commonality and Predominance – Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** This action involves common questions of law or fact, which predominate over any questions affecting individual Class members, including:

(a) whether Sony engaged in the wrongful conduct alleged herein;

(b) whether Sony owed a legal duty to Plaintiffs and the other Class members to exercise due care in collecting, storing, and safeguarding their Personal Information;

(c) whether Sony negligently or recklessly breached legal duties owed to Plaintiffs and the other Class members to exercise due care in collecting, storing, and safeguarding their Personal Information;

(d) whether Sony's conduct violated Cal. Civ. Code § 1750 *et seq.*;

(e) whether Sony's conduct violated Cal. Bus. & Prof. Code § 17200 *et seq.*;

(f) whether Sony's conduct violated Cal. Bus. & Prof. Code § 17500 *et seq.*;

(g) whether Sony's conduct violated Cal. Civ. Code § 1798.80 *et seq.*;

(h) whether Sony has been unjustly enriched through its acts and/or omissions alleged herein;

(i) whether Plaintiffs and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

(j) whether Plaintiffs and the other Class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

112. Sony engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

113. **Typicality – Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other Class members because, among other things, Plaintiffs and the other Class members were injured through the substantially uniform misconduct described above. Plaintiffs herein are advancing the same claims and legal theories on behalf of themselves and all other Class members, and there are no defenses available to Sony that are unique to Plaintiffs.

114. **Adequacy of Representation – Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class members they seek to represent; they have retained—and the Court has appointed—counsel competent and experienced in complex class action litigation; and Plaintiffs will prosecute this action vigorously. The Class' interests will be fairly and adequately protected by Plaintiffs and their counsel.

115. **Superiority – Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Sony, making it impracticable for Class members to individually seek redress for Sony's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments, and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties

and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

116. This is particularly true here, because Sony's "Terms of Service and User Agreement" mandates the application of California law to Plaintiffs' and the other Class members' claims.

CLAIMS ASSERTED

COUNT I

Violation of California's Unfair Competition Law ("UCL")

(Cal. Bus. & Prof. Code § 17200 *et seq*.)

117. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in Paragraphs 1-116 above, as though fully stated herein.

118. Sony engaged in unfair, unlawful, and fraudulent business practices in violation of the UCL.

119. By reason of the conduct alleged herein, Sony engaged in unlawful, unfair, and deceptive practices within the meaning of the UCL. The conduct alleged herein is a "business practice" within the meaning of the UCL.

120. Sony violated the UCL by misrepresenting the quality of its Network, specifically the security thereof, and its ability to safely store Plaintiffs' and the other Class members' Personal Information. Sony stated in its privacy policy that it would take "reasonable measures" to protect customers' Personal Information against breaches in security, but failed to do so. In violation of industry standards, Sony used weak or no encryption and failed to adequately install and maintain firewalls. Sony was aware of previous attempts to break into its systems but failed to rectify shortcomings in its security systems and technologies that allowed for those breaches and ensuing Data Breach to be successful.

121. Sony also violated the UCL by failing to immediately notify Plaintiffs and the other Class members of the Data Breach. If Plaintiffs and the other Class members had been notified in an appropriate fashion, they could have taken precautions to safeguard their Personal Information.

122. Sony misrepresented that access to the PSN was a feature of PS3s and PSPs. *See* http://us.playstation.com/ps3/features/ps3featuresnetwork.html (last visited on Jan. 31, 2012).

123. Sony misrepresented that online connectivity and corresponding ability to connect to Qriocity, SOE, and Third Party Services, such as Netflix, was a feature of PS3s and PSPs. *See* http://us.playstation.com/ps3/features/ps_ps3_connectivity.html (last visited on Jan. 31, 2012).

124. Sony's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Cal. Bus. & Prof. Code §17500 *et seq.*, Cal. Civ. Code §1750 *et seq.*, Cal. Civ. Code § 1798.80 *et seq.*, and its own Privacy Policy.

125. Sony's actions also constitute "unfair" business acts or practices because, as alleged above, *inter alia*, Defendants omitted material facts regarding its Network, and thereby offended public policy and engaged in immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury to consumers, including Plaintiffs and the other Class members. The gravity of Sony's conduct outweighs any potential benefits attributable to such conduct. And, there were reasonably available alternatives to further Sony's legitimate business interests, other than Sony's conduct described herein.

126. Sony's representations and other conduct induced Plaintiffs to purchase PS3s and/or PSPs, to purchase and/or register for Sony's Online Services, to provide Personal Information when purchasing and/or registering for Sony's Online Services, and to purchase content from the Network and the PlayStation Store. But for these deceptive acts and business practices, Plaintiffs would not have purchased PS3s and/or PSPs, or would not have paid the prices they paid for their PS3s and/or PSPs, and would not have prepaid for Third Party Services from or used through the Network.

127. Plaintiffs and the other Class members suffered injury in fact and lost money or property as the result of Sony's failure to secure Plaintiffs' and the other Class members' Personal Information that was stored on Sony's servers. As the result of the Data Breach, Plaintiffs' and the other Class members' Personal Information was compromised, they lost the unencumbered use of their passwords, their passwords were obtained by a third party without their consent, and they lost the use of Sony Online Services. Additionally, other applications and products that can only be used

through the Network were rendered worthless, because Plaintiffs and the other Class members were unable to access said features due to Sony's disabling of its Network.

128. The value of Plaintiffs' and the other Class members' PS3s and PSPs was diminished as the result of Sony's failure to secure Plaintiffs' and the other Class members' Personal Information and the corresponding taking down of Sony Online Services for an extended period of time.

129. Plaintiffs would not have registered/subscribed to Sony Online Services or provided Sony with their Personal Information had they known of Sony's failure to maintain adequate or reasonable security measures to protect their Personal Information in its possession. Additionally, access to the PSN was a substantial factor in Plaintiffs' purchasing of their PS3s.

130. As a result of Sony's violation, Plaintiffs and the other Class members are entitled to restitutionary and injunctive relief.

COUNT II

Violation of California's False Advertising Law ("FAL")

(Cal. Bus. & Prof. Code § 17500 *et seq.*)

131. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in Paragraphs 1-116 above, as though fully stated herein.

132. Sony engaged in deceptive and misleading advertising in violation of the FAL.

133. Sony violated the UCL by misrepresenting the quality of its Network, specifically the security thereof, and its ability to safely store customers' Personal Information. Sony stated in its privacy policy that it would take "reasonable measures" to protect customers' Personal Information against breaches in security, but failed to do so. In violation of industry standards, Sony used weak or no encryption and failed to adequately install and maintain firewalls. Sony was aware of previous attempts to break into its systems but failed to rectify shortcomings in its security systems and technologies that allowed for those breaches and ensuing Data Breach to be successful.

134. Sony misrepresented that access to the PSN was a feature of PS3s and PSPs. *See* http://us.playstation.com/ps3/features/ps3featuresnetwork.html (last visited on Jan. 31, 2012).

135. Sony misrepresented that online connectivity and corresponding ability to connect to Qriocity, SOE, and Third Parties Services, such as Netflix, was a feature of PS3s and PSPs. *See* http://us.playstation.com/ps3/features/ps_ps3_connectivity.html (last visited on Jan. 31, 2012).

136. Sony's representations and other conduct induced Plaintiffs to purchase PS3s and PSPs, to purchase and/or register for Sony Online Services, and to provide Personal Information when purchasing and/or registering for Sony Online Services or purchasing content from the Network or the PlayStation Store. But for these deceptive acts and business practices, Plaintiffs would not have purchased PS3s and/or PSPs, or would not have paid the prices they paid for their PS3s and/or PSPs, and would not have prepaid for Third Party Services from or used through the Network.

137. Plaintiffs and the other Class members suffered injury in fact and lost money or property as the result of Sony's failure to secure Plaintiffs' and the other Class members' Personal Information that was stored on Sony's Network. As the result of the Data Breach, Plaintiffs' and the other Class members' Personal Information was compromised, they lost the unencumbered use of their passwords, their password was obtained by a third party without their consent, and lost the use of Sony Online Services as the result of the Data Breach. Additionally, other applications and products that can only be used through the Network were rendered worthless, because Plaintiffs and the other Class members were unable to access said features due to Sony's disabling of its Network.

138. The value of Plaintiffs' and the other Class members' PS3s and PSPs was diminished as the result of Sony's failure to secure Plaintiffs' and the other Class members' Personal Information and corresponding taking down of the Network for an extended period of time.

139. Plaintiffs would not have registered/subscribed to Sony Online Services or provided Sony with their Personal Information had they known of Sony's failure to maintain adequate or reasonable security measures to protect their Personal Information in its possession. Additionally, access to the PSN was a substantial factor in Plaintiffs' purchasing of their PS3s.

140. As a result of Sony's violation of the FAL, Plaintiffs and the other Class members are entitled to an order enjoining Sony from continuing the deceptive advertising described herein.

Plaintiffs and the other Class members are also entitled to restitution for the economic harm they have suffered as a result of the diminution in value of their PS3s and/or PSPs; and prepaying for access to certain services on the PSN, Qriocity, SOE, and Third Party Services, such as Netflix. Plaintiffs and the other Class members also suffered economic harm on account of purchasing PS3 games that were advertised and promoted based on their extensive multiplayer features that are only accessible via the PSN, and the value of which was substantially reduced because Plaintiffs and the other Class members were unable to access said features due to Sony's disabling of the PSN.

COUNT III

Violation of California's Consumer Legal Remedies Act ("CLRA")

(Cal. Civ. Code § 1750 *et seq.*)

141. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in Paragraphs 1-116 above, as though fully stated herein.

142. The CLRA was enacted to protect consumers against unfair and deceptive business practices. It extends to transactions that are intended to result, or which have resulted, in the sale or lease of goods or services to consumers. Sony's acts, omissions, representations and practices as described herein fall within the CLRA because the design, development, and marketing of Sony's Equipment and Network services are intended to and did result in sales of PS3s, PSPs, and Network services.

143. Plaintiffs and the other Class members are consumers within the meaning of Cal. Civ. Code §1761(d).

144. Sony's acts, omissions, misrepresentations, and practices were and are likely to deceive consumers. By misrepresenting the safety and security of the Network, Sony violated the CLRA. Sony had exclusive knowledge of undisclosed material facts, namely, that its Network was defective and/or unsecure, and withheld that knowledge from Plaintiffs and the other Class members. Additionally, Sony misrepresented that a feature of PS3s and PSPs was access to the PSN.

145. Sony's acts, omissions, misrepresentations, and practices alleged herein violated the following provisions of the CLRA, which provides, in relevant part, that:

> (a) The following unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer are unlawful:
>
> > (5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have . . . .
> >
> > (7) Representing that goods or services are of a particular standard, quality, or grade . . . if they are of another.
> >
> > (9) Advertising goods or services with intent not to sell them as advertised.
> >
> > (14) Representing that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law.
> >
> > (16) Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

146. Sony stored Plaintiffs' and the other Class members' Personal Information on its Network. Sony represented to Plaintiffs and the other Class members that its Network was secure and that their Personal Information would remain private. Sony engaged in deceptive acts and business practices by providing in its Privacy Policy that it uses "reasonable measures to protect the confidentiality, security, and integrity of the personal information collected from [its] website visitors," and that it maintains security measures "to protect the loss, misuse, and alteration of the information under our control."

147. Sony knew or should have known that it did not employ reasonable measures that would have kept Plaintiffs' and the other Class members' Personal Information secure and prevented the loss or misuse of Plaintiffs' and the other Class members' Personal Information. For example, Sony failed to use a sufficient encryption code to protect Plaintiffs' and the other Class members' financial information and failed to employ any encryption to protect other personal information, such as email addresses and passwords.

148. Sony's deceptive acts and business practices induced Plaintiffs and the other Class members to purchase PS3s and PSPs, to purchase or register for Sony Online Services, and to provide Personal Information, including credit card information, for the purchase of content from the Network or the PlayStation Store. But for these deceptive acts and business practices, Plaintiffs and the other Class members would not have purchased PS3s, PSPs and/or prepaid for Third Party

Services from or used through the Network, or would not have paid the prices they paid for PS3s, PSPs, and/or Third Party Services from or used through the Network.

149. Sony's representations that access to the PSN was a feature of PS3s and PSPs and that it would secure and protect Plaintiffs' and the other Class members' Personal Information in its possession were facts that reasonable persons could be expected to rely upon when deciding whether to purchase PS3s, PSPs, Sony Online Services, and/or Third Party Services from or used through the Network.

150. Plaintiffs and the other Class members were harmed as the result of Sony's violations of the CLRA, because their Personal Information was compromised, placing them at a greater risk of identity theft; they lost the unencumbered use of their password; and their passwords were disclosed to third parties without their consent.

151. Plaintiffs and the other Class members suffered injury in fact and lost money or property as the result of Sony's failure to secure Plaintiffs' and the other Class members' Personal Information; the values of Plaintiffs' and the other Class members' PS3s and/or PSPs were diminished as the result of Sony's failure to secure Plaintiffs' and the other Class members' Personal Information and corresponding taking down of Sony Online Services for an extended period of time; and applications and products that can only be accessed through the Network were rendered worthless, because Plaintiffs and the other Class members were unable to access said features due to Sony's disabling of the Network.

152. Sony's conduct alleged herein was oppressive, fraudulent, and/or malicious, thereby justifying an award of punitive damages.

153. As the result of Sony's violation of the CLRA, Plaintiffs and the other Class members are entitled to compensatory and exemplary damages, an order enjoining Sony from continuing the unlawful practices described herein, a declaration that Sony's conduct violated the CLRA, restitution as appropriate, attorneys' fees, and the costs of litigation.

154. Pursuant to Cal. Civ. Code §1782, on June 8, 2011, Plaintiff Johnson mailed Sony notice in writing, via U.S. certified mail, of the particular violations of Cal. Civ. Code §1770 of the CLRA and demanded that Sony rectify the actions described above by providing complete

monetary relief, agreeing to be bound by Sony's legal obligations and to give notice to all affected customers of their intent to do so. Plaintiffs Johnson has not received a response from Sony and Sony has failed to take the actions demanded to rectify its violation of the CLRA. Therefore, Plaintiffs now seek damages for such unfair and deceptive practices pursuant to Cal. Civ. Code §1782.

COUNT IV

Violation of Cal. Civ. Code § 1798.80 *et seq.*

155. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in Paragraphs 1-116 above, as though fully stated herein.

156. Section 1798.82 of the California Civil Code provides, in pertinent part, as follows:

> (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
>
> (b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
>
> (c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.
>
> (d) Any person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:
>
> (1) The security breach notification shall be written in plain language.
>
> (2) The security breach notification shall include, at a minimum, the following information:
>
> (A) The name and contact information of the reporting person or business subject to this section.
>
> (B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

> (C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.
>
> (D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
>
> (E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
>
> (F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.
>
> * * *
>
> (f) Any person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.
>
> (g) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

157. The Data Breach constituted a "breach of the security system" of Sony.

158. Sony unreasonably delayed informing anyone about the breach of security of Plaintiffs' and other Class members' confidential and non-public information after Sony knew the Data Breach had occurred.

159. Defendants failed to disclose to Plaintiffs and other Class members, without unreasonable delay, and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Personal Information when they knew or reasonably believed such information had been compromised.

160. Upon information and belief, no law enforcement agency instructed Sony that notification to Plaintiffs or other Class members would impede investigation.

161. Pursuant to Section 1798.84 of the California Civil Code:

> (a) Any waiver of a provision of this title is contrary to public policy and is void and unenforceable.
>
> (b) Any customer injured by a violation of this title may institute a civil action to recover damages.
>
> (c) In addition, for a willful, intentional, or reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed three thousand dollars ($3,000) per violation; otherwise, the customer may recover a civil penalty of up to five hundred dollars ($500) per violation for a violation of Section 1798.83.
>
> * * *
>
> (e) Any business that violates, proposes to violate, or has violated this title may be enjoined.

162. As a result of Sony's violation of Cal. Civ. Code § 1798.82, Plaintiffs and the other Class members incurred economic damages relating to expenses for credit monitoring, loss of use and value of Sony Online Services, loss of use and value of prepaid Third Party Services, and diminution of the value of their PS3s and/or PSPs.

163. Plaintiffs, on behalf of themselves and the Class, seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to: (a) damages suffered by Plaintiffs and the other Class members as alleged above; (b) statutory damages for Sony's willful, intentional, and/or reckless violation of Cal. Civ. Code § 1798.83; and (c) equitable relief.

164. Plaintiffs also seek reasonable attorneys' fees and costs under Cal. Civ. Code §1798.84(g).

COUNT V

Unjust Enrichment

165. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in Paragraphs 1-116 above, as though fully stated herein.

166. Plaintiffs and the other Class members conferred benefits on Sony by paying for PS3s, PSPs, Qriocity, SOE, and related games, applications, products, and online services marketed and promoted for their multiplayer features available only through the PSN.

167. Plaintiffs and the other Class members, however, were deprived of the full value of their PS3, PSP, Qriocity, SOE, Third Party Services, and related games, applications, products, and online services due to Sony's disabling of Sony Online Services.

168. Sony knowingly and willingly accepted monetary benefits resulting from Plaintiffs' and the other Class members' purchases, but failed to honor its obligations to them. Rather, Sony benefited from Plaintiffs' and the other Class members' purchases of the aforementioned PS3s, PSPs, Qriocity, SOE, Third Party Services, and related games, applications, products, and online services, yet deprived Plaintiffs and the other Class members of the full use and value of these products and services.

169. Under the circumstances described herein, it is inequitable for Sony to retain the monetary benefits at the expense of Plaintiffs and the other Class members.

170. By engaging in the conduct described above, Sony has been unjustly enriched at the expense of Plaintiffs and the other Class members. Under the circumstances, it would be contrary to equity and good conscience to permit Sony to retain the ill-gotten benefits that Sony received in light of the violations of law detailed herein.

171. As the result of Sony's unjust enrichment, Plaintiffs and the other Class members have suffered injury and are entitled to reimbursement, restitution, and disgorgement by Sony of the benefit conferred by Plaintiffs and the other Class members.

COUNT VI

Negligence

172. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in Paragraphs 1-116 above, as though fully stated herein.

173. Sony owed a duty to Plaintiffs and the other Class members to exercise reasonable care in safeguarding and protecting their Personal Information in its possession from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Sony's security systems to ensure that Plaintiffs' and the other Class members' Personal Information in Sony's possession was adequately secured and protected. Sony further had a duty to implement processes that would detect a breach of its security system in a timely manner.

174. Sony had a duty to timely disclose to Plaintiffs and the other Class members that their Personal Information had been or was reasonably believed to have been compromised. Timely

disclosure was appropriate so that, among other things, Plaintiffs and the other Class members could take appropriate measures to avoid unauthorized charges to their credit/debit card accounts, cancel or change usernames and passwords on compromised accounts, and monitor their account information and credit reports for fraudulent activity.

175. Sony breached is duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Class members' Personal Information in its possession by failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and the other Class members' Personal Information; failing to adequately monitor the security of the Network; allowing unauthorized access to Plaintiffs' and the other Class members' Personal Information stored on the Network; and failing to recognize in a timely manner that the Network had been breached.

176. Sony breached its duty to timely disclose that Plaintiffs' and the other Class members' Personal Information in its possession had been, or was reasonably believed to have been, stolen or compromised.

177. Sony's failure to comply with industry regulations, such as PCI DSS, and the delay between the date of intrusion and the date Sony informed customers of the Data Breach further evidence Sony's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Class members' Personal Information in its possession.

178. But for Sony's wrongful and negligent breach of its duties owed to Plaintiffs and the other Class members, their Personal Information would not have been compromised, and Sony Online Services would not have been shut down for extended periods of time.

179. The injury and harm suffered by Plaintiffs and the other Class members was the reasonably foreseeable result of Sony's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Class members' Personal Information within its possession. Sony knew or should have known that its systems and technologies for processing and securing Plaintiffs' and the other Class members' Personal Information had security vulnerabilities.

180. As a result of Sony's negligence, Plaintiffs and the other Class members incurred economic damages relating to expenses for credit monitoring, loss of use and value of Sony Online

Services, loss of use and value of prepaid Third Party Services, and diminution of the value of their PS3s and/or PSPs.

COUNT VII

Bailment

181. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in Paragraphs 1-116 above, as though fully stated herein.

182. Plaintiffs and the other Class members delivered and entrusted their Personal Information to Sony for the sole purpose of accessing and using Sony Online Services and Third Party Services.

183. During the time of bailment, Sony owed Plaintiffs and the other Class members a duty to safeguard their Personal Information stored on its Network by maintaining reasonable security procedures and practices to protect such information. As alleged herein, Sony breached this duty.

184. As a result of Sony's breach of this duty, Plaintiffs and the other Class members have been harmed as alleged herein.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other Class members, respectfully request that this Court enter an Order:

A. Certifying the Class under Federal Rule of Civil Procedure 23(a) and 23(b)(3), appointing Plaintiffs as Class Representatives, and appointing their undersigned counsel as Class Counsel;

B. Finding that Sony's conduct was negligent, deceptive, unfair, and unlawful as alleged herein;

C. Enjoining Sony from engaging in the negligent, deceptive, unfair, and unlawful business practices alleged herein;

D. Awarding Plaintiffs and the other Class members actual, compensatory, and consequential damages;

E. Awarding Plaintiffs and the other Class members statutory damages;

F. Awarding Plaintiffs and the other Class members restitution and disgorgement;

G. Requiring Sony to provide appropriate credit monitoring services to Plaintiffs and the other Class members;

H. Awarding Plaintiffs and the other Class members exemplary damages, should the finder of fact determine that Sony acted with oppression, fraud, and/or malice;

I. Awarding Plaintiffs and the other Class members pre-judgment and post-judgment interest;

J. Awarding Plaintiffs and the other Class members reasonable attorneys' fees and costs, including expert witness fees; and

K. Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of all claims in this Consolidated Class Action Complaint so triable.

Dated: January 31, 2012

Respectfully submitted,

/s Paul J. Geller
ROBBINS GELLER RUDMAN & DOWD LLP
PAUL J. GELLER
120 E. Palmetto Park Road, Suite 500
Boca Raton, Florida 33432
(561) 750-3000

/s Adam J. Levitt
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
ADAM J. LEVITT
55 West Monroe Street, Suite 1111
Chicago, Illinois 60603
(312) 984-0000

/s Ben Barnow
BARNOW AND ASSOCIATES, P.C.
BEN BARNOW
One North LaSalle Street, Suite 4600
Chicago, Illinois 60602
(312) 621-2000

/s Brian R. Strange
STRANGE & CARPENTER
BRIAN R. STRANGE (103252)
12100 Wilshire Boulevard, Suite 1900
Los Angeles, California 90025
(310) 207-5055

/s David A. McKay
HERMAN GEREL, LLP
DAVID A. MCKAY
230 Peachtree Street, NW, Suite 2260
Atlanta, Georgia 30303
(404) 880-9500

Plaintiffs' Steering Committee

/s Timothy G. Blood
BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
600 B Street, Suite 1550
San Diego, California 92101
(619) 338-1100

Plaintiffs' Co-Liaison Counsel

/s Gayle M. Blatt
CASEY GERRY SCHENK FRANCAVILLA
BLATT & PENFIELD, LLP
GAYLE M. BLATT (122048)
110 Laurel Street
San Diego, California 92101
(619) 238-1811

CERTIFICATE OF SERVICE

I hereby certify that on January 31, 2012, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to the email addresses denoted on the Electronic Mail Notice List, and that I shall cause the foregoing document to be mailed via the United States Postal Service to the non-CM/ECF participants indicated on the Electronic Mail Notice List.

/s Ben Barnow

BARNOW AND ASSOCIATES, P.C.
BEN BARNOW
One North LaSalle Street, Suite 4600
Chicago, Illinois 60602
(312) 621-2000
b.barnow@barnowlaw.com